Information Theory, Spring 2018	Iftach Haitner

Problem set 4

May 7, 2018 — Due: May 24

- Please submit the handout in class, or email the grader (quefumas at gmail.com).
- Write clearly and shortly using sub-claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- It is allowed to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase")

1. Show that $\mathrm{SD}(p,q) = \max_{\mathcal{S}\subseteq[m]}\left(\sum_{i\in\mathcal{S}} p_i - \sum_{i\in\mathcal{S}} q_i\right)$ for any two distributions p, q over $[m]$.

2. Use the above to prove that $\mathrm{SD}(p,q) = \max_{\mathsf{D}}\left(\Pr_{X\sim p}[\mathsf{D}(X)=1] - \Pr_{X\sim q}[\mathsf{D}(X)=1]\right)$, where the max is over all deterministic distinguishers. Try and extend the above to randomized distinguishers?

3. Relative entropy is not symmetric: give two distributions p, q such that $D(p\|q) \neq D(q\|p)$, and $D(p\|q), D(q\|p) < \infty$.

4. Relative entropy does not obey the triangle inequality: give three distributions p_1, p_2, p_3 such that $D(p_1\|p_2) + D(p_2\|p_3) < D(p_1\|p_3)$

5. Relative entropy is non-negative: given two distributions p, q, show that $D(p\|q) \geq 0$, with equality only if $p = q$.

6. Does Theorem 4 in Lecture 7 hold for any prefix code C with $\mathrm{E}_{i\leftarrow q}[|C(i)|] \leq H(q) + 1$?

   (and not only for a code C with $C(x) = \left\lceil \log \frac{1}{q(x)} \right\rceil$, as stated in the theorem)

7. Prove the data processing inequality of relative entropy (Claim 7 in Lecture 7) for randomized functions.

8. Let $U_1, \ldots, U_k$ be uniform independent bits, let $\varepsilon > 0$ and let W be the event that at least $k(\frac{1}{2}+\varepsilon)$ of these bits are ones. Use Thm 10 in Lecture 7 to show that $\Pr[W] \leq 2^{-k\varepsilon^2}$. BTW, does this inequality look familiar to you?